# 要 約 書

被認証者は、乱数、ユーザＩＤ、パスワードを基に今回の認証データと次回の認証データを一方向性関数を用いて算出し、これをさらに排他的論理和を用いて今回と次回の両パラメータを関連づけした形で暗号化し、これらを被認証者自身のユーザＩＤと合わせて認証者に送信する。

認証者は、被認証者から前述の３つの情報を受信し、今回の認証データを基に一方向性関数を用いて算出した正当性確認パラメータと前回の認証フェーズにおいて登録した認証パラメータと比較し、一致したら今回の認証が成立したと判断し、次回の認証データを次回の認証パラメータとして登録する。